From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Date: Friday, September 16, 2022 3:52:18 PM

Hello,

Below are my comments addressing the questions posed on the solicitation.

Use of the CUI Series

1. How organizations are currently using the CUI series (SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A)
   A: I believe that organizations are primarily using the CUI series when they are required to by contract or solicitation. DFARS 7012 is a major contributor to organizations using the CUI series. Without compulsion, I do not believe organizations would use the CUI series. In my opinion, contractors typically will only do what is required of them and do not go beyond that without additional compulsion.

2. How organizations are currently using the CUI series with other frameworks and standards (e.g., NIST Risk Management Framework, NIST Cybersecurity Framework, GSA Federal Risk and Authorization Management Program [FedRAMP], DOD Cybersecurity Maturity Model Certification [CMMC], etc.)
   A: Same as above, only when required to. RMF is a separate requirement that covers government information systems or contractor systems operated on behalf of the government. CMMC Level 2 has become 1:1 with 800-171 until revision 3, when there will likely end up being a lag period for the DoD to update the CMMC model. Contracts typically will specify the version of 800-171 required, so those contracts will need contract modifications with additional money for contractors to implement the delta between revisions, or they will be addressed at re-compete and solicitation to include the latest version of 800-171. FedRAMP's main goal is to speed up adoption of cloud at government agencies by allowing reciprocity of ATO decisions. DoD is attempting to add scope to FedRAMP by requiring non-traditional CSPs to obtain FedRAMP or pay for expensive annual 3PAO attestation statements. Neither are a good option and are an expansion of FedRAMP scope. CSF is talked about at a high level but that's really the involvement that I have seen about it at various organizations, with the exception of critical infrastructure, they have taken to CSF more than any other organizations.

3. How to improve the alignment between the CUI series and other frameworks
   A: I would recommend 800-171 and the protections for CUI become an overlay using 800-53 controls instead, and then organizations can select the minimally required controls from the overlay and then select any additional controls they want for integrity and availability for their own purposes, not regulatory compulsion, using the same catalog of controls. That seems more streamlined to me and also allows for easier discussions of interconnections between contractor systems and government information systems that use 800-53. It would

be straight apples to apples when evaluating security of interconnection security agreements. Putting which CSF phase a control in 800-53 is part of might be an interesting way to show more linkage between RMF and CSF.

4. Benefits of using the CUI series

   A: It is a good starting point for security programs and has some flexibility within it, the requirements are little more clearly written than 800-53 controls which are typically intentionally ambiguous to allow for flexibility in implementations and not pointing to one solution. 800-171 could take a 800-161 approach where it takes the 800-53 controls and adds additional context to them.

5. Challenges in using the CUI series

   A: 800-171 as originally written is good guidance. The problem is when other agencies take the guidance and then it changes into mandatory and strict pass/fail exercises like CMMC 1.0 tried to do. The best example of how this would fail is with the requirements for FIPS 140 validated modules. CMMC 1.0 did not allow POA&Ms and CMMC 2.0 is projected to allow POA&Ms for 6 months. Resolving FIPS issue is going to take more than 6 months. Priority sometimes has to be given to security vulnerability patches and not staying on outdated versions just because they have the FIPS validation and the newer version does not have that validation yet. So a strict adherence to 800-171 could lead to major vulnerabilities in order to stay in compliance with the FIPS 140 requirement.

Updates for consistency with SP 800-53 Revision 5 and SP 800-53B

6. Impact on the usability and existing organizational implementation (i.e., backward compatibility) of the CUI series if it were updated for consistency with SP 800-53 Revision 5 and the moderate security control baseline in SP 800-53B

   A: By using 800-53 controls instead of 800-171 requirements, and by using a CUI overlay for the selection of CUI controls, then this need for consistency is immediately resolved. An interesting side effect is that a federal information system could choose to use the CUI overlay for confidentiality if the system they have does not care about integrity of availability requirements. In the inverse, a contractor organization can select from the entire 800-53 catalog for any additional controls they would want to select and tailor for their environment.

Updates to improve usability and implementation

7. Features of the CUI series should be changed, added, or removed. Changes, additions, and removals can cover a broad range of topics, from consistency with other frameworks and standards to rescoping criteria for inclusion of requirements. For example:
   a. Addition of new resources to support implementation: The benefits and challenges of including an SP 800-53 Control Overlay [1] and/or a Cybersecurity Framework Profile Appendix as an alternative way to express the CUI security requirements.

      A: I support this. The CUI series could be absorbed as an overlay. One overlay for 171 and a separate overlay for 172.

b. Change to the security requirement tailoring criteria: Impact of modifying the criteria used to tailor [2] the moderate SP 800-53B security control baseline (e.g., the potential inclusion of controls that are currently categorized as *NFO – Expected to be routinely satisfied by nonfederal organizations without specification*)

   A: Not including NFOs was overly optimistic. NFOs have to be included if you want contractors to do NFOs. They only do what is required of them. NFO have to be required explicitly with the associated determination statements for verification and validation.

8. Any additional ways in which NIST could improve the CUI series

   A: Clarification on 1.1 statement of applicability for "The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." Specifically, the last clause could use more clarification on what the requirements are for components that provide security but do not process/store/transmit CUI themselves. This has caused some heartburn and confusion for CMMC and increased scope of applying all 800-171 requirements to components that provide a minimal protection and do not have CUI.

V/R

Dr. Jeff Baldwin
CISSP-ISSAP-ISSEP, CCSP, CISM, CISA, PMP
CEO, Space Coast Cybersecurity LLC
[redacted]